

Abstract (Basic): JP 11175474 A

NOVELTY - A password management apparatus maintains login ID and user password . During effective login condition, a thyme password previously generated along with unique security code, is included in the HTML page of user service, generated dynamically. During next access, when the thyme password is detected to be effective, accessing of corresponding function of web server is approved.

USE - For authenticating user to access web servers in internet

ADVANTAGE - Enables maintenance of data without including any document in management directory of web server. Prevents inaccurate usage of web server, reliably.

Dwg.1/1

Title Terms: USER; AUTHENTICITY; SYSTEM; CONTROL; ACCESS; WEB; SERVE; ACCESS; CORRESPOND; FUNCTION; WEB; SERVE; THYME; PASSWORD; DYNAMIC;

GENERATE; PAGE; USER; SERVICE; DETECT; EFFECT

Derwent Class: T01

International Patent Class (Main): G06F-015/00

File Segment: EPI

Manual Codes (EPI/S-X): T01-J

BEST AVAILABLE COPY

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-175474

(43) 公開日 平成11年(1999) 7月2日

(51) Int.Cl.⁶

G 0 6 F 15/00

識別記号

3 3 0

F I

G 0 6 F 15/00

3 3 0 B

審査請求 未請求 請求項の数5 書面 (全 4 頁)

(21) 出願番号

特願平9-369746

(22) 出願日

平成9年(1997)12月10日

(71) 出願人 393020889

マシンコントロールシステム有限会社

東京都品川区西大井4丁目21番10号

(72) 発明者 田中 雅男

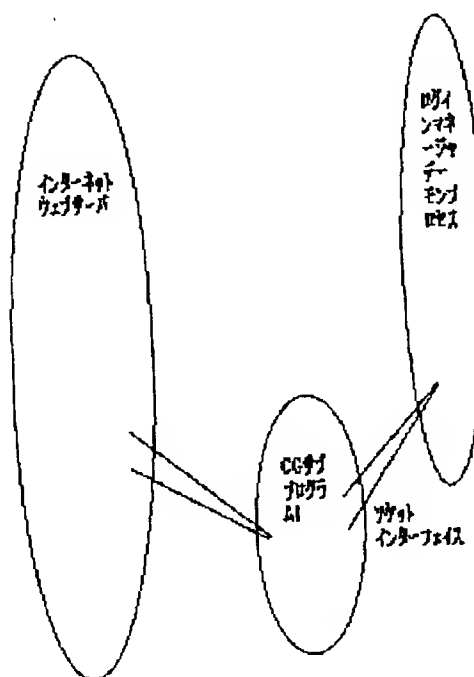
東京都品川区西大井4丁目21番10号

(54) 【発明の名称】 ウェブサーバ用ログインマネージャ

(57) 【要約】

【課題】ウェブサーバの不正使用を防止するセキュリティ管理と課金管理をすることが可能なログイン技術を提供する。

【解決手段】ユニークなセキュリティコードを発生するワンタイムパスワード発生装置と、ログインIDとユーザパスワードを管理するパスワード管理装置と、前記変換されたワンタイムパスワードとを連携づけ、有効なログイン状態である場合に前記ワンタイムパスワードに対応する機能の実行を許可するセキュリティ管理処理部とをウェブサーバのコンピュータ本体に備えるものである。



【特許請求の範囲】

【請求項1】ウェブサーバのログインにおいて、ユニークなセキュリティコードを発生するワнтаイムパスワード発生装置とログインIDとユーザパスワードを管理するパスワード管理装置と、前記変換されたワнтаイムパスワードとを連携づけ、有効なログイン状態である場合に、前記ワнтаイムパスワードを動的に生成するユーザサービスのHTMLページ中に埋め込み、次回のアクセス時に、有効なワнтаイムパスワードであるかどうかを検査することにより、ログイン状態の維持を管理する機能をコンピュータ本体にそなえる装置である。

【請求項2】ウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワнтаイムパスワードにより、ユーザ認証されるため、その認証されたページ処理の課金情報ログを残し、その課金情報ログをもとに、定期的に、課金集計し、ウェブサーバシステムにおいて、アクセスページ単位の課金請求を実現する装置である。

【請求項3】請求項1の装置を実現する方式。

【請求項4】請求項2の装置を実現する方式。

【請求項5】ウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワнтаイムパスワードにより、ユーザ認証されるため、ウェブサーバの管理ドキュメントディレクトリ外に置かれたコンテンツを動的にウェブサーバの管理ドキュメントディレクトリ内に転送して、コンテンツの配布管理を実現する装置である。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】本技術は、ウェブサーバのセキュリティをワнтаイムパスワードに応じてウェブサーバが管理する特定の機能の実行を許可するコンピュータ不正使用防止装置に適用して有効な技術に関するものである。

【0002】

【従来の技術】近年、インターネットのウェブサーバを使用した業務が増加するにつれて、ユーザに関する課金や重複ログインに関して、ウェブサーバで管理したい状況になっている。

【0003】従来のウェブサーバに蓄積されたデータの内、コンピュータの利用者の利用資格を確認し、コンピュータの不正使用を防止するユーザ認証には、パスワードを使用するベーシック認証が一般的である。

【0004】前記ベーシック認証を使用する方法は、利用者を識別するユーザIDと利用者本人しか知ることができないパスワードをウェブサーバが管理しているURL配下のディレクトリに対して、アクセスする許可をURL単位に認証している。

【0005】前記ウェブサーバとウェブブラウザの通信は、HTTP通信プロトコルによる、コネクションレス

プロトコルを利用する方法である。

【0006】

【発明が解決しようとする課題】前記従来技術を検討した結果、以下の問題点を見出した。

【0007】前記ベーシック認証でURLを認証する方法では、時系列的に見た場合、ある人のログイン処理をコンピュータがおこなっている時に、同一人物、あるいは別人が同じパスワードを使いログインした場合、後者のログイン認証の重複検査ができない。そのため、ユーザごとに検索履歴などの個人情報を壊す可能性があり、ある時間軸の中で、同一IDに対して、多重ログインを阻止したいが、ベーシック認証ではできない。

【0008】前記HTTP通信プロトコルは、コネクションレスプロトコルのため、ログイン後のページからアクションされ、動的に生成されたページからさらにアクションをしていくような同一ログインで時間的連続性を保証するような要求を処理するためには、動的に作成されたページ中にログインした個人を識別するなんらかの識別子を埋め込む必要がある。しかし、ログインIDやユーザのパスワードは、識別子にはなるが、これは個人の機密情報であるため、再利用される可能性のあるページ中にユーザパスワードを入れることはできない。

【0009】動的に作成されたページがどのユーザがログインし生成したかを保証することにより、生成したページ単位に課金処理をおこないたい要求がある。

【0010】本技術の目的は、コンピュータの不正使用を防止するセキュリティ管理の操作性を向上する事が可能な技術を提供することにある。

【0011】本技術の他の目的は、ログイン後にそのユーザが動的に生成するページにセキュリティの確保されたワнтаイムパスワードを埋め込むことにより、個人の機密情報であるユーザパスワードを隠蔽し、かつコンピュータ側ではログイン後のユーザを識別できる技術を提供することにある。

【0012】本技術の他の目的は、静的なコンテンツをウェブサーバの管理外ディレクトリに置き、コンテンツ配布プログラムを経由して、動的にコンテンツを配布するコンテンツ配布管理ができる技術を提供することにある。

【0013】本技術の他の目的は、ログイン後にそのユーザが静的あるいは動的に生成するページのアクセスにおいて決められた単価で課金する従量課金システムの技術を提供することにある。

【0014】

【課題を解決するための手段】本技術によって開示される発明のうち、代表的なものを説明すれば、下記のとおりである。

【0015】(1)ウェブサーバのログインにおいて、ユニークなセキュリティコードを発生するワнтаイムパスワード発生装置とログインIDとユーザパスワードを

管理するパスワード管理装置と、前記変換されたワнтаイムパスワードとを連携づけ、有効なログイン状態である場合に、前記ワнтаイムパスワードを動的に生成するユーザサービスのHTMLページ中に埋め込み、次のアクセス時に、有効なワнтаイムパスワードであるかどうかを検査することにより、ログイン状態の維持を管理する機能をコンピュータ本体にそなえる装置である。

【0016】(2)前記(1)に記載されたウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワнтаイムパスワードにより、ユーザ認証されるため、その認証されたページ処理の課金情報ログを残し、その課金情報ログをもとに、定期的に、課金集計し、ウェブサーバシステムにおいて、アクセスページ単位の課金請求を実現する装置である。

【0017】(3)前記(1)に記載されたウェブサーバ用ログインマネージャ装置において、ログイン以後は、各ページのアクセスは、毎回ワнтаイムパスワードにより、ユーザ認証されるため、ウェブサーバの管理ドキュメントディレクトリ外に置かれたコンテンツを動的にウェブサーバの管理ドキュメントディレクトリ内に転送して、コンテンツの配布管理を実現する装置である。

【0018】

【実施例】(実施形態1)以下、本発明のウェブサーバ用ログインマネージャについて説明する。

【0019】図1は、本実施形態のウェブサーバ用ログインマネージャの概略構成を示す図である。

【0020】本ウェブサーバ利用者は、まず本システム利用に先立ち、サービス事務局より、利用資格として、ユーザIDとパスワードを発行してもらうことが必要です。

【0021】サービス事務局より発行するユーザIDとパスワードは、ログインマネージャのパスワード管理処理部に登録します。

【0022】利用者は、サービス事務局より発行されたユーザIDとパスワードを使いログインページのURLから、ログインマネージャのCGI処理部に入ってきます。

【0023】このCGI処理部は、ログインマネージャデーモンプロセスとソケット通信を行い、ログインプロトコルでログインの要求を送ります。

【0024】ログインマネージャデーモンは、送られてきたユーザIDとパスワードが、パスワード管理処理部に登録されているかをデータベースをサーチして確認します。

【0025】パスワード管理処理の結果登録ユーザである場合は、ワнтаイムパスワード発行処理部でワнтаイムパスワードを発生させて、ユーザIDとワнтаイムパスワードを関連づけ、ログインマネージャデーモンプロセスで、管理するアクティブリストに登録し、アクティ

ブリスト監視タイマーで定期検査します。

【0026】その結果を呼び出したプロセスに通知し、登録ユーザであれば、ログインマネージャデーモンプロセスから渡されたワнтаイムパスワードを保持しながら、CGI処理部のページ処理機能を実行して、実際の利用者へのサービスを提供し、そのサービスの結果である利用者へ返すページにワнтаイムパスワードのみをHTMLのヒドン属性に埋め込んで返します。

【0027】また、このCGI処理部で、アクセスログと課金ログを保存して、以後のアクセス集計管理とユーザ毎の課金請求処理データになります。

【0028】また、このCGI処理部で、ウェブサーバの外側に置かれた静的なコンテンツをウェブサーバの管理するドキュメントディレクトリにコピーし、配布を管理する機能も処理可能である。

【0029】登録ユーザでない場合は、ログインエラー処理で利用者に通知。

【0030】ワнтаイムパスワードの埋め込まれた動的処理用のページから呼び出されるCGI処理部は、ワнтаイムパスワードを、ログインマネージャデーモンプロセスに通信することにより、アクティブリストにワнтаイムパスワードが登録されているかどうかを検査して、結果をCGI処理部へ返します。

【0031】ウェブサーバから起動される、CGIサブプログラムは、ワнтаイムパスワードを利用したログインマネージャデーモンからのセッション検査機能により、どのページからのアクセスが、どの利用者からのページであるかをログインマネージャデーモンからの結果をもとに判断し、ワнтаイムパスワードによるウェブサーバから発生するページ毎にユーザ認証する方式の装置です。

【0032】(実施形態2)以下、本発明のウェブサーバ用ログインマネージャの課金処理機能について説明する。実施形態1の中で、個人認証されたページ単位の課金ログ情報を定期的(月末処理)に集計することで、各ユーザID単位で、アクセスページとそのページ処理単価で、課金集計プログラムで処理することで、従量課金などの細かな請求処理データを作成することが可能である。

【0033】

【作用および効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【0034】(1)ウェブサーバのログインにおいて、1個人が1時期において、多重にログインする排他制御が可能になるため、1個人ごとのアクセス履歴を残す事が可能である。

【0035】(2)ページアクセスの毎に、ユーザ認証が取れているため、課金すべきページに対して、従量課金をすることが、可能である。

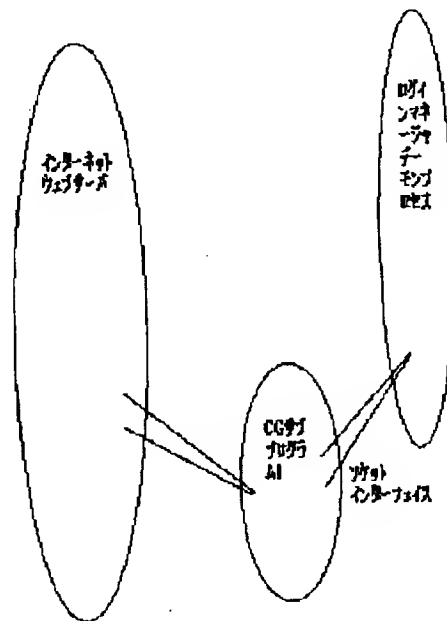
【0036】(3) 静的なドキュメントでも、動的にコンテンツを配布することが可能になるため、ウェブサーバの管理ディレクトリにドキュメントを置かずに、データを保持することが可能なため、コンテンツ配布用プログラムを経由せずには、ウェブサーバからアクセスでき

ないため、コンテンツを動的に管理することが可能になる。

【図面の簡単な説明】

【図1】本実施形態の概略構成図

【図1】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.